The Polish Bomba and the Turing-Welchman Bombe

The Polish Bomba

The leading Polish cryptanalysts were Marian Rejewski, Jerzy Różycki and Henryk Zygalski. In 1938 they developed the first codebreaking machine, called the "Bomba kryptologiczna". The name was supposedly taken from the ice cream Bombe. Already before they had built a *cyclometer* from two Enigmas. The Polish codebreakers made their knowledge and experience available to the British.

The electromechanical Bombe

In 1940 the mathematician *Alan Turing* designed an electromechanical machine, the *Turing Bombe* (see Figs. 1–2). The effectiveness of the first version was however unsatisfactory. The machine interrupted the automatic search when a possible Enigma wheel position was found, necessitating many manual interventions.

The mathematician *Gordon Welchman* proposed incorporating additional circuits. These were called the diagonal board. With these one could simultaneously test the circuit inputs and outputs. This vastly improved the cracking of the Enigma and accelerated the process considerably.

The Bombes had 36 rotors. The improved machine was also called the *Turing-Welchman Bombe*.

The purpose of the Bombe was to support the efforts to decrypt the secret radio messages of the Nazis generated with the aid of the *Enigma* cryptographic machine. From 1940 to 1945 the Bombes determined the respective *rotor sequence* (wheel order) of the Enigma daily key. This was an essential prerequisite for the decoding that followed. Thus, the Turing-Welchman Bombe did not transform the unintelligible messages into understandable communications, but provided the basis for the codebreaking process. Thanks to the procedure now available, the ciphertexts could then be transferred by hand to plain language with the British *Typex* cryptographic machines and translated into English. These machines, which had five rotors, emulated the Enigmas. The device, also called the Type X, was manufactured from 1937 (Model 1) and 1938 (Model 2). The coding and decoding machine was modified for cracking the Enigma messages.

The mathematician *Peter Twinn* unveiled the circuitry of the Enigma. For breaking the ciphertexts the capture of code books was also a decisive factor.

Irvin Good, a colleague of Turing, remarks:

> "I won’t say that what Turing did made us win the war, but I dare say we might have lost it without him" (see Raymond Kurzweil: The age of intelligent machines, MIT press, Cambridge, Massachusetts 1990, page 175).

There were several code names for the Turing-Welchman Bombe (see Table 1):

Table 1: The various versions of the Turing-Welchman Bombe

The three versions of the Turing-Welchman Bombe			
Code name	**Delivered**	**Number**	**Remarks**
Victory	March 18 1940	1	Disappointing performance because of too many false interruptions
Agnus dei (Agnes), Spider	August 8 1940	>200	Excellent performance thanks to additional circuits proposed by Gordon Welchman
Jumbo	End of 1941	few	Further circuits for the automatic suppression of certain interruptions
© Bruderer Informatik, CH-9401 Rorschach, Switzerland 2022			

Remarks

211 Bombes were manufactured, of which six were in Bletchley Park and the others in remote locations.

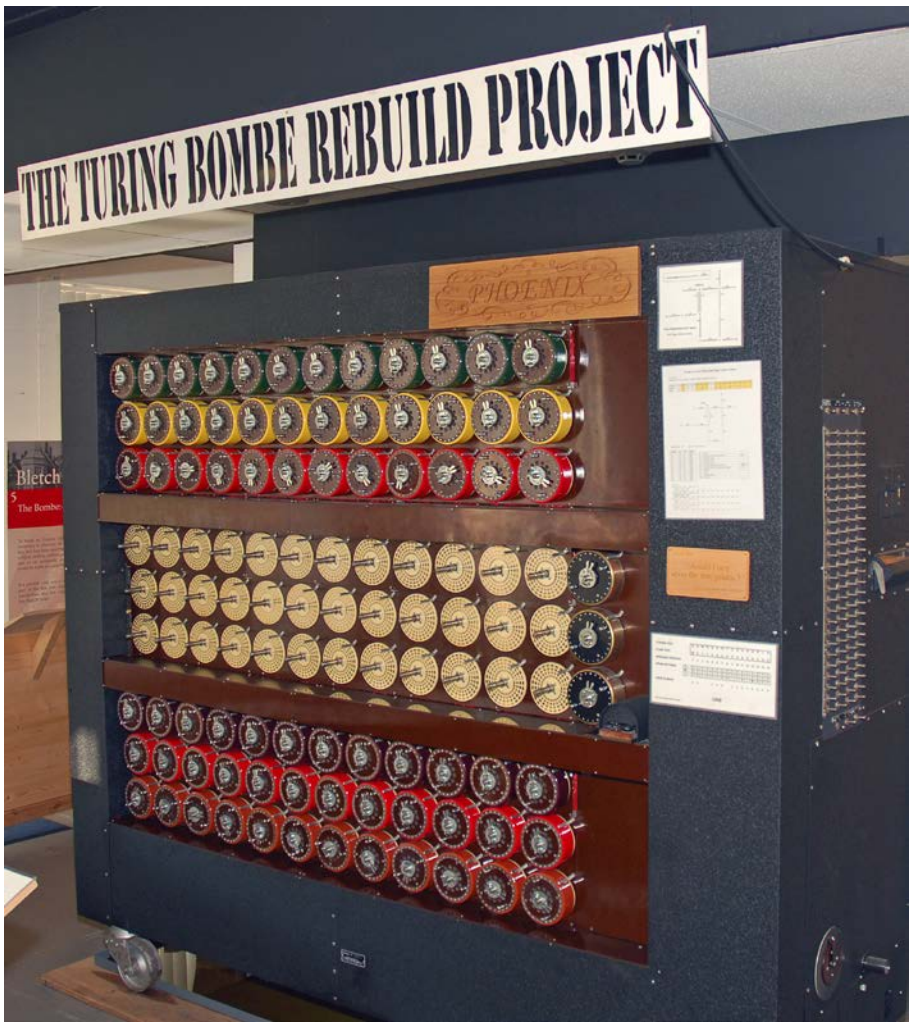


Fig. 1: Front side of the Turing-Welchman Bombe. This three rotor Turing Bombe is a functional rebuild (3 x 12 units on each of 3 rotors). More than 200 of these were used in the Second World War to crack the German Enigma (©Turing Welchman Bombe Rebuild Trust, Bletchley Park).

Remark

The Turing-Welchman Bombe is located in the National Museum of Computing in Bletchley Park.

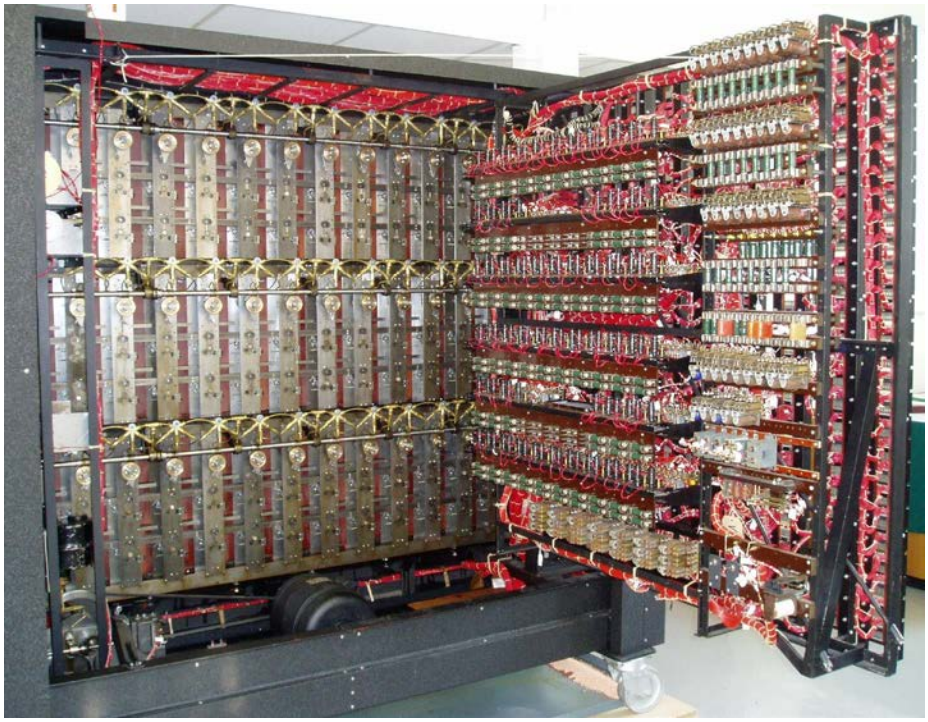


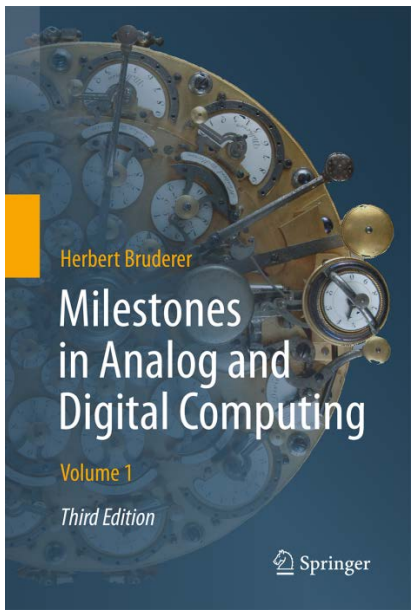
Fig. 2: Rear view of the Turing-Welchman Bombe. This photo shows the internal workings of the machine designed by Alan Turing and improved by Gordon Welchman. The Bombes are regularly demonstrated in Bletchley Park (©Turing Welchman Bombe Rebuild Trust, Bletchley Park).

Sources

Herbert Bruderer: Milestones in Analog and Digital Computing, Springer Nature Switzerland AG, Cham, 3rd edition 2020, 2 volumes, 2113 pages, 715 illustrations, 151 tables, translated from the German by John McMinn, https://www.springer.com/de/book/9783030409739

Frank Carter: The Turing Bombe, Bletchley Park Trust, Bletchley Park, Milton Keynes 2008

Brian Oakley: The first break into German Enigma at Bletchley Park, Bletchley Park Trust, Bletchley Park, Milton Keynes 2011.



Meilensteine der Rechentechnik/Milestones in Analog and Digital Computing, volume 1 (Credit: De Gruyter Oldenbourg/Springer Nature 2020)

Bruderer, Herbert: Meilensteine der Rechentechnik, De Gruyter Oldenbourg, Berlin/Boston, 3. Auflage 2020, Band 1, 970 Seiten, 577 Abbildungen, 114 Tabellen, https://www.degruyter.com/view/title/567028?rskey=xoRERF&result=7

Bruderer, Herbert: Meilensteine der Rechentechnik, De Gruyter Oldenbourg, Berlin/Boston, 3. Auflage 2020, Band 2, 1055 Seiten, 138 Abbildungen, 37 Tabellen, https://www.degruyter.com/view/title/567221?rskey=A8Y4Gb&result=4

Herbert Bruderer
Seehaldenstrasse 26
Postfach 47
CH-9401 Rorschach
Switzerland
+41 71 855 77 11
herbert.bruderer@bluewin.ch,
bruderer@retired.ethz.ch

December 2022